

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

----- X
E*TRADE FINANCIAL CORPORATION and :
E*TRADE SECURITIES LLC, :
:

Plaintiffs, :
:

v. :
:

No. 08 CV 2993 (RJH)
:

MARCUS J. HERNANDEZ, :
SEAN J. GAFFEY, and :
BANC OF AMERICA :
INVESTMENT SERVICES, INC. :

Defendants. :
----- X

**DECLARATION OF JEFFERY A. WIMER
IN FURTHER SUPPORT OF E*TRADE'S REPLY MEMORANDUM**

JEFFERY A. WIMER declares as follows pursuant to 28 U.S.C. § 1746:

1. I am employed by E*TRADE Securities LLC ("E*TRADE") as Branch Manager, Retail Branch, at 135 East 57th Street, 12th Floor, New York, NY 10022 ("New York branch"). I make this further declaration in support of E*TRADE's Reply Memorandum.

Response to Hernandez Declaration

2. Beginning in February 2007, I supervised Marcus Hernandez ("Hernandez") at E*TRADE's New York branch.

3. As I stated in my first declaration, on November 19, 2007, Hernandez e-mailed to his home e-mail account eight spreadsheets containing client information from E*TRADE's computer system.

4. On November 19 or November 20, 2007, Hernandez transferred from the New York branch to another fully operational E*TRADE branch at 150 Allendale Road, King of Prussia, PA 19406-2926.

5. I understand that Hernandez now claims that he e-mailed these spreadsheets to his home e-mail because (1) he was concerned about his “immediate computer and email access” in his new Pennsylvania office (Hernandez Decl. ¶ 6), (2) that he did it as a “precaution,” and (3) that “it is not a violation of any firm policy to email such materials to a personal email account for work purposes.” ¶ 6.

6. A review of E*TRADE’s computer security policy (“Computer Policy”) shows Hernandez’s claims to be false. They are also illogical on their face based on E*TRADE’s computer network configuration.

7. E*TRADE’s Computer Policy requires users to store “Customer Confidential” information on shared, secure network drives that are regularly backed up. The policy also prohibits individuals from storing client information on their local computers and from sending client information externally unless it is first encrypted. Hernandez violated company policy and endangered client confidentiality by storing client information on his desktop computer and then e-mailing unencrypted client lists to his home e-mail address. (E*TRADE Financial Corp., *Corporate Information Security: Information Security ALL USERS’ Policy* at 6, 19, 21, 22 relevant sections attached hereto as Ex. 1).

8. E*TRADE’s Computer Policy automatically appears periodically on all internal E*TRADE computer users’ screens and requires users to pledge compliance with it.

9. E*TRADE’s Computer Policy was incorporated into Hernandez’s Employment Agreements by E*TRADE’s Code of Professional Conduct (“Code”). The Code required

Hernandez to “adhere to all Company policies and any policies that your business unit or department may set governing such usage.” (Wimer 3/25/2008 Decl. ¶ 18, Ex. 3 at 24). The Code expressly formed part of the terms and conditions of Hernandez’s employment. (Wimer 3/25/2008 Decl. ¶ 18, Ex. 3 at 4). Hernandez acknowledged the that he was bound by the terms of the Code both in his signed Acknowledgments of the Code (Wimer 3/25/2008 Decl. ¶¶ 25-26, Exs. 6 & 7), and also by signing his offer letter, which provided that the Code constituted part of his employment agreement. (Wimer 3/25/2008 Decl. ¶ 22, Ex. 4).

10. E*TRADE records show that Hernandez completed computer policy training on November 2, 2004; June 19, 2006; and December 10, 2007.

11. Hernandez violated E*TRADE’s Computer Policy merely by storing the client lists on his desktop work computer.

12. All E*TRADE network data is available from all E*TRADE computers in each E*TRADE location using proper login information. Thus, if Hernandez had complied with E*TRADE’s computer use policy and saved this client information to the E*TRADE network, he could have accessed this information from any computer on the E*TRADE network. To access this client information, Hernandez only needed to log onto any computer workstation at the King of Prussia branch or any other E*TRADE office. With this ready access to E*TRADE’s network, Hernandez had no legitimate reason to export client information to his home e-mail account.

13. Also, Hernandez had no legitimate reason to compile E*TRADE client information. E*TRADE representatives are required to access client information through a web-based program known as Genie that runs on E*TRADE’s internal computer network. Hernandez should have used Genie to access client information as part of his daily interaction with clients.

14. Hernandez also violated E*TRADE's Code of Professional Conduct by e-mailing the client information to his home e-mail account. E*TRADE policy provides that client information should not be taken outside of the office except with authorization: "Generally, information made available through E*TRADE FINANCIAL's intranet is intended for internal use only." (See E*TRADE Financial Corp., *Code of Professional Conduct* at p. 25, attached as Ex. 3 to Wimer 3/25/2008 Decl.).

15. Hernandez had no authorization to take E*TRADE financial information outside of the office. Hernandez never informed me that he was taking client information outside of the office in any form, and he never informed me that he was e-mailing client contact information to any non-E*TRADE e-mail account. I never gave Hernandez authorization or permission to take client contact information outside the office or to send the information to a non-E*TRADE e-mail account.

16. Finally, Hernandez's excuses for sending client information to his personal e-mail account are illogical. Since any E*TRADE employee can log in from any E*TRADE computer, there is no legitimate concern about computer and e-mail access at a new branch. However, even if Hernandez had truly been concerned about "immediate computer and e-mail access" after his transfer to the King of Prussia branch office, he would have sent the files to his friend and future branch manager, Matthew Ellis, instead of violating policies by sending it to his home e-mail address.

Response to Gaffey Declaration

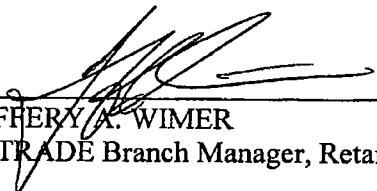
17. Sean Gaffey's ("Gaffey") declaration falsely suggests that I gave him permission to violate his Employment Agreement, E*TRADE's Code of Professional Conduct and the law by encouraging him to take E*TRADE's client information. (Decl. ¶ 4). This is all false.

18. Gaffey claims in his Declaration that we discussed that he would need to retain E*TRADE client information in any anticipated move and also claims that I told him he would need to transfer his clients to any new firm. Contrary to any assertion Gaffey makes in his Declaration, I repeatedly told him that, based on my experience, if he contacted E*TRADE's clients after leaving E*TRADE, he should be prepared for the consequences. I meant that the departed firm often takes legal action in these circumstances.

19. Gaffey's claims also make no sense. First, these statements would have been against my own economic interests because the departure of clients for whom my branch is responsible could reduce my compensation. Second, my understanding is that Banc of America Investment Services provides newly hired investment advisors such as Gaffey with client contacts and leads, so there would be no need to take his E*TRADE clients to a new position at Banc of America Investment Services.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge.

Executed this 14th day of April, 2008, at New York, New York.



JEFFERY A. WIMER
E*TRADE Branch Manager, Retail Branch

359385v2•RE

EXHIBIT 1



Corporate Information Security
Confidential

Corporate Information Security: Information Security ALL USERS' Policy

I. INTRODUCTION.....	2
1.1 INTRODUCTION.....	2
1.2 SCOPE.....	2
1.3 COMPLIANCE WITH POLICY.....	3
1.4 VIOLATION OF POLICY.....	3
II. SECURITY STRATEGIES AND PRINCIPLES.....	3
2.1 SECURITY STRATEGIES.....	4
2.2 SECURITY PRINCIPLES.....	4
III. SECURITY ROLES AND RESPONSIBILITIES.....	6
3.1 GENERAL ROLES AND RESPONSIBILITIES.....	6
3.2 INFORMATION SECURITY SUPPORT ROLES AND RESPONSIBILITIES.....	8
IV. USER MANAGEMENT GUIDELINES.....	9
4.1 INFORMATION ACCESS.....	9
4.2 USER ID POLICIES AND GUIDELINES.....	10
4.3 COMMON USER IDENTIFICATION NAMING STANDARDS.....	10
4.4 PASSWORD MANAGEMENT.....	12
4.5 LOGIN AND LOGOUT CONTROLS.....	14
4.6 ACCESS AND REVOCATION POLICY.....	15
V. SYSTEM MANAGEMENT GUIDELINES.....	18
5.1 ACCEPTABLE USE OF COMPUTER SYSTEMS.....	18
5.2 ACCEPTABLE USE OF THE INTERNET.....	19
5.3 ACCEPTABLE USE OF ELECTRONIC MAIL.....	20
5.4 INSTANT MESSAGING.....	22
5.5 BLOGGING POLICY.....	22
5.6 WIRELESS NETWORKING.....	22
5.7 WIRELESS KEYBOARD POLICY.....	23
5.8 SOFTWARE COPYING POLICY.....	23
5.9 PERSONAL COMPUTER BACK UP POLICY.....	23
5.10 VIRUS PROTECTION POLICY.....	24
5.11 CELLULAR COMMUNICATION POLICY.....	26
5.12 REMOTE ACCESS POLICY.....	27
5.13 ENCRYPTION POLICY.....	28
5.14 PHYSICAL ACCESS POLICIES.....	29
5.15 DATA, DOCUMENTS AND E-MAIL RETENTION, ELECTRONIC AND PAPER.....	30
5.16 CUSTOMER DATA USE IN DEVELOPMENT & TESTING.....	30
5.17 EMBEDDED LINKS IN EMAIL COMMUNICATIONS.....	30
VI. SUMMARY OF SIGNIFICANT FEATURES.....	30
VII. POLICY REVISION HISTORY.....	31
VIII. BOARD OF DIRECTORS ACCEPTANCE HISTORY.....	33
IX. POLICY ACKNOWLEDGEMENT FORM.....	34



1.3 COMPLIANCE WITH POLICY

The policies, procedures and guidelines described in this manual are not optional. Every E*TRADE FINANCIAL Employee is expected to comply fully with all requirements. Failure to comply may result in disciplinary action, up to and including termination. In addition, civil or criminal legal action may be pursued as appropriate.

Contingent Workers who enjoy a business relationship with E*TRADE FINANCIAL are also expected to fully comply with all applicable information security policies, procedures and guidelines. Failure to comply may result in termination of the business relationship between E*TRADE FINANCIAL and Contingent Workers. Compliance with E*TRADE FINANCIAL policies may relate directly or indirectly to federal, state, and local legal or regulatory requirements. It is E*TRADE FINANCIAL's intent to be in full compliance with all legal and regulatory requirements. Further, E*TRADE FINANCIAL will pursue legal remedies (civil and criminal) where warranted, to ensure compliance with policy.

1.4 VIOLATION OF POLICY

Violation of E*TRADE FINANCIAL Information Security Policies, Procedures and Guidelines should be brought to the immediate attention of the Help Desk or Information Security Management.

The Information Security Team will work with appropriate managers to ensure the problem is resolved and to address necessary steps to eliminate future violations. Information Security Administration will consult with Human Resources to determine what, if any, disciplinary action will be taken by E*TRADE FINANCIAL with respect to the violation. Human Resources must approve and manage, in conjunction with the violating Employee's manager, any disciplinary action taken.

The Help Desk should be called to report system issues including, but not limited to:

- Actual or suspected virus infections
- Loss or theft of system access tokens
- Loss or theft of computer hardware

Information Security Management should be called to report security policy, procedures and guidelines issues and violations including, but not limited to:

- Compromise or disclosure of sensitive information
- Compromise or disclosure of passwords
- Compromise of system controls
- Any violation of E*TRADE FINANCIAL's Information Security Policies, Procedures and Guidelines

II. SECURITY STRATEGIES AND PRINCIPLES

There are several security strategies that support the protection of information assets. Where practical, policies, procedures and guidelines should be developed using the following strategies.



2.1 SECURITY STRATEGIES

2.1.1 Accountability

All persons who use E*TRADE FINANCIAL information are personally responsible for exercising proper control over classified information. Policies, procedures and guidelines are developed to ensure that the use of classified information is monitored and individuals are accountable for their actions. Outside consultants, contractors, and temporary workers are subject to the same security requirements and responsibilities as E*TRADE FINANCIAL's Employees.

2.1.2 Need To Know

Classified information is shared with individuals on a need-to-know basis. This strategy requires that access to information be commensurate with job responsibilities and requirements.

2.1.3 Policy Awareness

The success of any policy, procedure or guideline is directly related to employees' knowledge of the requirements. Awareness programs are required to ensure that requirements are known and understood. The awareness extends to the Board of Directors, to which reports are made annually.

2.2 SECURITY PRINCIPLES

The following principles are the foundation for E*TRADE FINANCIAL information security policies. These principles are guidelines, used to ensure that E*TRADE FINANCIAL's information assets will be protected from unauthorized disclosure, and are available for business requirements and accurate in order to support the company's business objectives. There are four components that describe E*TRADE FINANCIAL's Security Principles:

2.2.1 Information Ownership

Each type of information asset is owned by a specific E*TRADE FINANCIAL Employee who has the ultimate authority to establish the business purpose for the information. The owner classifies the information, approves access to the information, and determines requirements for retention of the information within regulatory and company guidelines.

Customer information is defined as any record containing information about an individual in his or her capacity as a customer or prospective customer, whether in paper, electronic, or other form, that E*TRADE FINANCIAL maintains or that is maintained on E*TRADE FINANCIAL's behalf. There are references throughout this policy to "information assets" which include customer information.

2.2.2 Information Classification

Information has varying degrees of sensitivity. Disclosure and protection of information is governed by the classification assigned to the information. The owner of the information determines information classification and labels it accordingly. There are three (3) levels of classification associated with information:

- **CUSTOMER CONFIDENTIAL DATA:**

CUSTOMER CONFIDENTIAL DATA is defined as E*TRADE FINANCIAL customers' private information and its disclosure represents the highest level of risk to the company. Customer confidential data must be protected from unauthorized disclosure. Unauthorized disclosure would result in a responsibility to inform customers of that disclosure and could adversely impact E*TRADE FINANCIAL's ability to do business. Because E*TRADE FINANCIAL Employees are also customers and have privacy rights, employee confidential data also falls into this category and should be afforded the same protection as customer confidential data. Examples of data included in this classification



Corporate Information Security Confidential

level are: customer and employee private data, account numbers, social security numbers, account balances, etc.

Customer Confidential includes Customer Non-Public Information (CNPI). CNPI is defined as identifying information including Customer Name, Social Security Number, Tax ID, Address Location, Account Number, Credit Card Number, Driver's License Number, User ID and any other data unique to a customer.

- **COMPANY SENSITIVE DATA:**
COMPANY SENSITIVE DATA is defined as information that has no restrictions on disclosure within the company. This information could have an adverse impact on E*TRADE FINANCIAL if disclosed outside the company and should be secured appropriately, depending on the level of sensitivity. Examples of this classification may include technical drawings, company financial information that is non-public, Intranet web page news, phone directories or organization charts, business plans, etc.
- **NON-SENSITIVE DATA:**
NON-SENSITIVE DATA is defined as information that is not classified in either the Customer Confidential or Company Sensitive categories. This information is routine, short term, day-to-day information and is freely discussed. Disclosure of non-sensitive information has no foreseeable adverse impact on E*TRADE FINANCIAL or its ability to conduct business or its customers. Non-sensitive information does not need to be labeled. Examples of this classification may include published news stories, publicized company events, website offerings, etc.

2.2.3 Information Classification Matrix

Classification	Customer Confidential	Company Sensitive
Characteristics	<ul style="list-style-type: none"> • Customer and Employee Non-Public Information • Unauthorized disclosure would adversely impact E*TRADE FINANCIAL's ability to do business • Unauthorized disclosure would require notification to customers 	<ul style="list-style-type: none"> • Provides E*TRADE FINANCIAL with a competitive edge • Potentially harmful to E*TRADE FINANCIAL if disclosed • Restricted use within the company • Sensitive to personnel, technical, or business endeavors
Examples	<ul style="list-style-type: none"> • Customer and Employee Account Numbers • Social Security Numbers • Customer account balance information 	<ul style="list-style-type: none"> • All information stored or printed from computers unless otherwise specified • Organizational Charts • Telephone Directories • Network Diagrams • Salary Information • Acquisition Plans • Non-public financial information • Logon Credentials
Disclosure	<ul style="list-style-type: none"> • To Employees on a need-to-know basis • To outside entities after signing a non-disclosure agreement 	<ul style="list-style-type: none"> • To Employees on a need-to-know basis. • Outside sources on a need-to-know basis.
Copying	<ul style="list-style-type: none"> • Only when required to perform job function • Only when copy is afforded same security measures as original 	<ul style="list-style-type: none"> • No Restrictions Within E*TRADE FINANCIAL
Telephone	<ul style="list-style-type: none"> • Only after taking reasonable 	<ul style="list-style-type: none"> • No Restrictions Within



Corporate Information Security Confidential

	steps to ensure identity of the other party	E*TRADE FINANCIAL
Physical Security	<ul style="list-style-type: none"> Stored in secure manner when not in use 	<ul style="list-style-type: none"> No Restrictions Within E*TRADE FINANCIAL
Internal Mail	<ul style="list-style-type: none"> Envelope with classification labeled on outside 	<ul style="list-style-type: none"> No Restrictions Within E*TRADE FINANCIAL
External Mail	<ul style="list-style-type: none"> Envelope with classification labeled on outside 	<ul style="list-style-type: none"> No Restrictions Within E*TRADE FINANCIAL
Destruction	<ul style="list-style-type: none"> Destroy beyond reconstruction 	<ul style="list-style-type: none"> No Restrictions Within E*TRADE FINANCIAL

All data classified as "**Customer Confidential**" or "**Company Sensitive**" must be encrypted during transmission between remote sites. Appropriate facilities, hardware, or PC software mechanisms will be approved and provided by E*TRADE FINANCIAL to allow Employees to meet this requirement.

2.2.4 Security Awareness

Each E*TRADE FINANCIAL Employee has an obligation to protect the information assets of the company and to ensure that the information is used for appropriate business purposes. Employees are required to complete the online Security Awareness training module and to acknowledge receipt of and compliance with security policy annually in order to ensure that requirements are known and understood.

It is the responsibility of management to ensure that all users of information understand how to protect company assets, including information and information resources, and comply with security policies, procedures and guidelines. Supervisors and managers must ensure that persons working within their business units understand general information protection requirements and are sufficiently knowledgeable about the Information Security Policies, Procedures and Guidelines. Supervisors and managers must recognize the need for protecting information and the requirements for which they are specifically responsible.

III. SECURITY ROLES AND RESPONSIBILITIES

3.1 GENERAL ROLES AND RESPONSIBILITIES

Information Security Management Policies give management an infrastructure to systematically implement security controls that maintain a desired level of information *integrity, confidentiality, and continuity*. An important component of the Information Security Policy is the definition of personnel responsibilities. Each person who deals with information has responsibilities in determining how they should handle information. Responsibilities are defined for Employees (information users), Information Owners, Managers and the Information Security Team.

3.1.1 Employee Responsibilities (Information Users)

Information users include all Employees of E*TRADE FINANCIAL who access or receive information produced, stored, or communicated by E*TRADE FINANCIAL's information technology systems. Information users also include all individuals who, by virtue of their relationship with E*TRADE FINANCIAL (e.g., contractors, vendors, service providers, consultants, temporary Employees, etc.) are entrusted with sensitive or confidential information. All users must:



Corporate Information Security
Confidential

4.6.2.5 Certification of Access

It is important that both access and permission levels be reviewed and certified on a periodic basis. Periodically, Access Control will provide access lists to application owners and/or reporting managers of critical systems in accordance w/ the Application Accounts Audit Procedure maintained by Corporate Information Security. It is the responsibility of the owners and managers to review the access list for accuracy. Information Owners and managers must advise Access Control of any required changes to the access and capabilities of individuals. Access Control will modify or delete access as indicated by the information owner or manager via the MAC process.

There are two critical components to the certification process: (1) Access to information by specific individuals must be validated and (2) Specific capabilities must be reviewed for each individual.

Individuals (including contractors, consultants, agency temporaries and business partners) that are no longer employed by E*TRADE FINANCIAL or no longer have a business requirement must be identified and their access revoked.

4.6.2.6 Temporary Access

Temporary access is often granted to external users such as consultants, vendor personnel, temporary Employees, etc. and for special projects or to resolve technical problems. Special controls should be used to provide the prompt suspension/deletion of a temporary user access when the contract or project expires. Automatic expiration of temporary user access should be used where possible. Otherwise, special manual administration and audit procedures are required. Individuals responsible for requesting temporary access must identify a specific end date for the temporary user. If the expiration period needs to be extended, a MAC form must be submitted requesting the extension beyond the specified date.

V. SYSTEM MANAGEMENT GUIDELINES

5.1 ACCEPTABLE USE OF COMPUTER SYSTEMS

Achievement of E*TRADE FINANCIAL business objectives is significantly aligned with appropriate use of computer resources. Communication of information internally and availability of information externally is a fundamental requirement for the continued success of E*TRADE FINANCIAL business activities.

E*TRADE FINANCIAL has made a substantial investment in computer resources. In order to protect these resources and to ensure that each E*TRADE FINANCIAL Employee, business partner and customer receives maximum benefit from computer resources, it is expected that the use of computer resources be consistent with the highest standards of professionalism, ethical conduct and integrity.

Each E*TRADE FINANCIAL Employee is expected to comply fully with all requirements. Failure to comply may result in whatever action E*TRADE FINANCIAL deems appropriate, up to and including termination.

The following are the minimum requirements for the use of E*TRADE FINANCIAL computer resources and do not represent the complete list of requirements:



Corporate Information Security Confidential

- E*TRADE FINANCIAL computers, workstations and associated equipment must be used only for authorized company business.
- Any activity must conform absolutely to the strictest legal and regulatory requirements. This includes license requirements for all software.
- Attempts to gain unauthorized access to information or capabilities are prohibited.
- Unauthorized disclosure of Customer Confidential or Corporate Sensitive information is prohibited.
- Unauthorized modification of E*TRADE FINANCIAL computers, networks and software is prohibited.
- Loading unauthorized personal software on to E*TRADE FINANCIAL computers or workstations are prohibited.
- Access to all E*TRADE FINANCIAL computer networks and environments must be made only with approved workstations and laptops.
- Access to and from all E*TRADE FINANCIAL computer networks and environments must be made only through approved access points. Non-approved modem or wireless network connections are prohibited.
- Using another individual's account or user's identification is not allowed.
- Initiating or forwarding chain e-mail is not allowed.
- The use of profanity, racial comments, implied or explicit sexual comments or inappropriate religious comments will not be tolerated in any communication associated with E*TRADE FINANCIAL.
- All individuals are expected to maintain the confidentiality of their passwords.
- All individuals must ensure that their computer is protected from inappropriate use when unattended by either logging off or ensuring that the computer is password protected.
- All individuals must follow departmental procedures to back up and maintain company information.
- All control procedures established to safeguard and maintain E*TRADE FINANCIAL computer environments and capabilities must be followed. Circumventing these established procedures is prohibited.
- All media used for copying Customer Confidential or Corporate Sensitive information must be clearly marked with the information classification and properly secured.
- All E*TRADE FINANCIAL critical information or data classified information as Customer Confidential or Corporate Sensitive information created or maintained on an individual workstation must be backed up or saved to a Local Area Network (LAN) server directory. This information must not be maintained on the workstation "C" drive.

The requirements and rules listed above are intended to serve as the minimum set of standards related to individual responsibility for E*TRADE FINANCIAL computer resources. Good judgment and common sense applies to this responsibility. If there are questions related to appropriate use, contact Information Security Administration.

5.2 ACCEPTABLE USE OF THE INTERNET

E*TRADE FINANCIAL, as a technology enabled corporation, recognizes the potential and opportunity associated with Internet use to facilitate achievement of business objectives. E*TRADE FINANCIAL encourages Employees to use the Internet appropriately in support of business objectives. While there are significant benefits that may be realized by Internet use, there are also risks that must be understood and managed. The intent of this policy is to establish guidelines for acceptable business use of the Internet.

- Network and information security issues require that Internet access be allowed through authorized access points protected by an E*TRADE FINANCIAL firewall. The E*TRADE



Corporate Information Security Confidential

FINANCIAL Firewall Policy describes the administration, control, procedures and monitoring of services allowed via the corporate firewall.

- The fundamental principle related to the firewall policy is that unless explicitly allowed, services are not permitted. This concept requires that specific services required for business use of the Internet such as Telnet, File Transfer Protocol (FTP), and other services be documented and approved in advance by the Vice President of the business area requiring the service, the Vice President of Technical Operations and Information Security Administration.
- Connectivity to the Internet is intended to support business objectives. As such, Internet use may be monitored for appropriate use. Periodic reports of Internet activity are made available to management for analysis and business requirement compliance. All requirements associated with Acceptable Use of Computer Systems apply to Internet use.
- The Internet represents a corporate presence and communication link to E*TRADE FINANCIAL customers and the general public. As such, all Internet use must conform to the standards of conduct expected of all E*TRADE FINANCIAL Employees.
- Any information exported to the Internet from E*TRADE FINANCIAL sources is owned by E*TRADE FINANCIAL. Exported information must be reviewed and approved by management prior to distribution.
- Any information imported from the Internet must conform to all legal, copyright and license requirements. Additionally, appropriate care must be taken to ensure imported information is from known sources and is virus free. Imported files must be scanned for viruses.
- Under normal circumstances, information exported via the Internet may be viewed by individuals outside the control of E*TRADE FINANCIAL. Extreme caution must be exercised to ensure that confidential or sensitive information is not sent over the Internet in an unsecured manner.
- Personal, non-business use of E*TRADE FINANCIAL networks and computer capabilities for unauthorized Internet purposes is prohibited.

Before users release any internal Company information, enter into any contracts, or order any products via public networks, the identity of the individuals and organizations contacted should be confirmed. Identity confirmation is ideally performed via digital signatures, but in cases where these are not yet available, other means such as letters of credit, third party references, and telephone conversations may be used. In addition, contracts are not to be entered into without express approval from Legal Affairs (see the Legal Affairs department web page on Channel*E for specific protocols regarding contracts at E*TRADE FINANCIAL). Products should be ordered through Purchasing whenever possible.

Unless the Chief Information Officer and Information Security Management has approved in advance, users are prohibited from using Internet connections to establish new or different business channels. These channels include electronic data interchange (EDI) arrangements, electronic mails with on-line shopping, on-line database services, etc.

5.3 ACCEPTABLE USE OF ELECTRONIC MAIL

Electronic mail (email) capabilities facilitate communications and represents an essential tool for achieving E*TRADE FINANCIAL business objectives. Email capabilities are provided to Employees to assist in carrying out the company's business. The email system allows Employees to communicate with each other internally and with individuals or business partners outside the company. This policy describes the ability of authorized E*TRADE FINANCIAL individuals to access, review, or disclose email messages sent or received by E*TRADE FINANCIAL Employees. This policy contains examples of acceptable use of the E*TRADE FINANCIAL email system. A more complete list of acceptable and unacceptable use of



Corporate Information Security Confidential

E*TRADE FINANCIAL's email can be found by reviewing the E*TRADE FINANCIAL Code of Professional Conduct.

5.3.1 Business Use

The electronic mail system is provided for business use. You may use the email systems for limited personal use in accordance with policies governing communications and conduct which can be found in the E*TRADE FINANCIAL Code of Professional Conduct. The Company treats all messages sent, received or stored in the email system as business messages.

Employees must be aware that messages created and stored on the Company's email systems are considered to be the property of E*TRADE FINANCIAL and are not granted privacy protection under the 1986 Electronics Communications Privacy Act. Furthermore, the SEC and other regulators impose various requirements on E*TRADE FINANCIAL or its subsidiaries regarding the preservation of "books and records," including email.

5.3.2 E*TRADE FINANCIAL Access, Review, Deletion and Disclosure

E*TRADE FINANCIAL can access, review, copy and delete any messages sent, received or stored on the email system. E*TRADE FINANCIAL has the right to access, review, copy or delete all such messages for any purposes and to disclose them to any party (inside or outside the company) it deems appropriate. Personal messages will be treated no differently from other messages (i.e., E*TRADE FINANCIAL reserves the right to access, review, copy, delete or disclose personal messages for any purpose). Employees must be aware that all messages are available for review by any authorized representative of E*TRADE FINANCIAL for any purpose.

5.3.3 Classified Company Information

Employees must exercise caution in transmitting company-classified information via the email system. Under most circumstances, email is inherently insecure and can be intercepted by unauthorized individuals. Additionally, email may be forged or modified, making the source and content of messages untrustworthy. **Customer Confidential and Corporate Sensitive information should never be transmitted or forwarded outside the company via unsecure email.** Customer Confidential and Corporate Sensitive information should never be transmitted or forwarded to individuals outside the company that are not authorized to receive that information and should not be sent or forwarded to other Employees inside the company who do not need to know the information.

Due to the insecure nature of external email, company data, email, or documents should not be forwarded to external email accounts, including Employee's own external accounts. Users that require email or data access while out of the office must use one of the approved methods of remote access listed in Section 5.12 Remote Access Policy.

5.3.4 Appropriate Use

Employees must be aware that email messages may be read by someone other than the addressee and may be disclosed to outside parties, including counsel, a regulatory body, or a court in connection with litigation or under a regulatory inquiry or investigation. Accordingly, care must be taken to ensure that messages are courteous, professional, and businesslike. The following list includes examples of appropriate use of email:

- To avoid telephone tag.
- To comment on a document or issue related to the business of E*TRADE FINANCIAL.
- To make a record of an instruction or request.
- To promulgate information to groups or individuals regarding an E*TRADE FINANCIAL business purpose.
- To allow individuals to effectively prioritize and manage time.



Corporate Information Security Confidential

A more complete list of acceptable and unacceptable use of E*TRADE FINANCIAL's electronic mail can be found by reviewing the Human Resources Policy.

5.3.5 Use of External Mail Systems

Unless expressly authorized by your business unit officer and Corporate Information Security, you may not use or access a personal e-mail account with an Internet Service Provider (ISP) or any other third party for any email. Among other considerations, regulatory requirements and anti-virus controls require the Company to forbid the use of such accounts.

5.4 INSTANT MESSAGING

The use of instant messaging (IM), chat, or peer-to-peer (P2P) client software on E*TRADE FINANCIAL's networks is restricted to only those installations performed by the IT organization and approved by Corporate Information Security. In accordance with the E*TRADE Code of Professional Conduct, all communications are subject to logging and administrative monitoring.

E*TRADE FINANCIAL's Instant Messaging Standard can be found on the official E*TRADE FINANCIAL intranet site and forbids the use of any IM, Chat, or Peer-to-Peer software which connects to peers or servers outside of the E*TRADE FINANCIAL network. All non-approved IM or Peer-to-Peer clients discovered on E*TRADE machines will be considered rogue software installations. Rogue clients found will be subject to immediate deletion, disconnection of the machine from E*TRADE FINANCIAL's network, and management notification. IM clients installed on non-E*TRADE FINANCIAL machines will be blocked while users are connected to the company's network.

5.5 BLOGGING POLICY

E*TRADE FINANCIAL respects the rights of individuals who may wish to express themselves through personal Web sites and Web logs commonly referred to as "blogs". Such forms of expressions may also include, but are not limited to, discussion forums, newsgroups, and collaboration tools, such as wikis.

While the company encourages such self-expression, Employees must respect the company's confidential and proprietary information. Any company sensitive data, customer confidential data and other financial information about the company shall not be disclosed to the public through any medium.

Further details and guidelines can be found under the HR Blogging Policy on Channel*E.

Should you have any questions on what may or may not be appropriate to include in "blogs", please discuss with Corporate Communications.

5.6 WIRELESS NETWORKING

No wireless networking equipment may be used on any E*TRADE FINANCIAL network or property unless approved by Corporate Information Security.

Approved wireless solutions are implemented with technology from Fortress Technologies. The approved solution requires the installation of a client on the user's laptop and must be approved by the business manager or higher. There is no requirement specified for access points or Wireless cards since the Fortress solution will work with any vendor. Currently, the following sites have approved solutions deployed: Irvine, Arlington, NY, Menlo Park, and the ROC – Alpharetta.

The E*TRADE Secure Wireless Standard requires that any wireless device must support Layer 2 encryption, and have that encryption permanently enabled. Approved wireless devices will be allowed on the network subject to design review and approval. Wireless devices found on the E*TRADE FINANCIAL network that do not comply with the approved wireless solutions list will be



Corporate Information Security Confidential

considered rogue, and will be subject to immediate shutdown, permanent removal from the network, and management notification.

Users that are issued E*TRADE FINANCIAL laptops should only use approved wireless solutions while on E*TRADE FINANCIAL campuses. Users should never connect to an unapproved wireless network while also connected to an E*TRADE FINANCIAL network. A request to use a wireless card while on E*TRADE FINANCIAL campuses requires a MAC request listing the business reason and must be approved by the requestor's business manager, Desktop Services and Corporate Information Security.

5.7 WIRELESS KEYBOARD POLICY

No wireless keyboard equipment may be used on any E*TRADE FINANCIAL network or property unless approved by Corporate Information Security. Any approved wireless keyboard solutions will be listed in the E*TRADE FINANCIAL purchasing system. Wireless keyboards found on the E*TRADE network that do not comply with the approved wireless keyboard solutions list will be subject to immediate shutdown, permanent removal from the network, and management notification.

5.8 SOFTWARE COPYING POLICY

Company-owned computers, workstations and approved software are intended to support business requirements, increase productivity and allow Employees to efficiently perform their jobs. It is company policy that only approved and authorized software can be copied or installed on E*TRADE FINANCIAL computer systems. This policy is necessary for several reasons:

Copied software significantly increases the risk of virus attacks. While virus protection schemes and software products are available and in use at E*TRADE FINANCIAL, significant threats exist that new virus attacks will occur and cause significant interruption to business activities.

Non-approved software does not support authorized business objectives. Games or other non-business software do not constitute appropriate use of company time.

E*TRADE FINANCIAL does not condone or tolerate software piracy. Copying software in violation of a license agreement is illegal. Reproducing or downloading software or media files (for example, music or video files) without authorization violates U.S. and international copyright laws and can subject both the company and individual employees to serious legal consequences. Unless Corporate Information Security personnel has been provided with a copy (electronic or otherwise) of a license for the employee's or company's use of copyrighted material, and the employee has a business purpose for using such material, employees are not permitted to download, copy or transfer software or media files using E*TRADE FINANCIAL's network or computers.

Non-approved software and media files discovered on E*TRADE FINANCIAL machines or servers will be deleted immediately.

5.9 PERSONAL COMPUTER BACK UP POLICY

Information stored on personal computers is a valuable asset. This information may include licensed software applications and programs, data files or other types of information used to meet business objectives. The value of this information is dependent on many factors including the criticality of the information, its usefulness in fulfilling job requirements, the time and effort to create or recreate the information and other factors related to maintaining and using the information.



Corporate Information Security Confidential

There are potential threats related to the loss of this information. Information stored on personal computers may be lost due to hardware failure, theft, inadvertent error, virus attacks, or other events that may cause the information to be destroyed or corrupted. In some cases, lost information may represent significant cost to E*TRADE FINANCIAL and may not be retrievable. To reduce the risk of information loss and to ensure recovery with the minimum disruption to business activities, information back-ups are required. The personal computer information back-up requirements described below represent the minimum acceptable standards.

The responsibility to ensure backups of information stored on individual personal computers rests with the creator of the information. Information that is lost or damaged can be recovered if appropriate backup procedures are performed.

For critical and sensitive information created or maintained on workstations which are connected to the E*TRADE FINANCIAL network, storing files in a directory located on a network file server will ensure that backups will automatically occur on a daily basis. Employees may save information to network file servers by placing the information on their "H" drive or by storing on a network drive. Information stored on a workstation's "C" drive is not backed up automatically. Employees must not store company critical or sensitive information on their "C" drive. For certain portable computers, network access may not be possible. In cases where it is not possible to save information to network file servers for automatic back up, critical or sensitive information must be backed-up manually to diskette or other media on a regular basis. The backed up information must be securely stored.

Each manager must ensure that information created by individuals in their area of responsibility is adequately protected from loss or corruption by an appropriate back-up plan. The back-up plan should include an inventory of critical or sensitive information that must be protected. The back-up plan and inventory should be coordinated with the Business Recovery Plan.

5.9.1 Desktop and Workgroup Services Group

The Desktop and Workgroup Services group is responsible for selecting and maintaining software and hardware to automatically back up all E*TRADE FINANCIAL file servers on a scheduled basis. The specific back-up methodology implemented must allow recovery of any file stored on any network file server. Details of the back-up methodology and a restoration plan must be documented. Testing of the back-up process must be accomplished on a periodic basis by retrieving specific files from the back-up media.

5.9.2 Information Security Administration

Information Security Administration is responsible for implementing awareness programs to ensure that backup requirements are met. Additionally, Information Security Administration will periodically test network backup procedures by requiring restoration of selected files. Compliance with this policy is subject to standard audit procedures and periodic security assessments.

5.10 VIRUS PROTECTION POLICY

The following policy has been developed to protect E*TRADE FINANCIAL from the loss of time and data associated with virus infections to company computer equipment. Computer viruses are a class of rogue programs designed to, at best, serve as a prank or, at worst, destroy a computer's operating system. Regardless of their intent, computer viruses adversely impact productivity and information. This policy is intended to serve as a guideline for Employees to significantly lessen the risk of virus infection.



Corporate Information Security Confidential

- All systems must be under the management of the Corporate Admin Account and Information Security Accounts. Removing these admin accounts from the local admin group is prohibited.
- All Employees must be aware of the threat that viruses represent. The real cost of viruses is not only the damage caused by a virus to either software or information, but also the cost of recovery. This cost includes the value of lost hours by the technical staff during recovery and the hours lost by Employees that are unable to work with infected applications or information. Awareness is the first step in preventing virus damage.
- Employees must contact the Help Desk when they suspect their computer has been infected with a virus. Each E*TRADE FINANCIAL workstation must be equipped with virus protection software that will indicate possible infection. When there is an indication that a virus is present, the Employee should immediately stop using their workstation and contact the Help Desk. Under no circumstances should the Employee continue to work on the infected workstation until instructed to do so by the Help Desk or Technical Support.
- Employees should perform virus scans on any software media that is loaded into the workstation. This virus scan requirement includes all diskettes, including new diskettes or CDs in "shrink-wrapped" packages, media transferred internally within E*TRADE FINANCIAL, and any storage media.
- Employees are also required to perform a virus scan on all a software and files downloaded from external sources including the Internet and vendor sites.
- Department managers must encourage Employees to report evidence of viruses on their workstations. Infection could occur from a disk brought in from home or from the prohibited use of non-authorized software. However, it is much better to report and eradicate a virus infection than to ignore it.
- Many virus 'warnings' are hoaxes and should not be distributed to other employees. All such 'warnings' should be sent to the Anti-Virus Team at "#AntivirusTeam.exchange.etrade.com" for verification and action if necessary.

5.10.1 Help Desk

- The Help Desk serves as the focal point for the coordination of eradication of all virus infections.
- The Help Desk will serve as the source of information for methods of dealing with viruses. The Desktop and Workgroup Services Group is responsible for actual procedures related to virus eradication and prevention. However, all actions will be communicated through the Help Desk.
- The Help Desk will deal with each virus incident promptly.
- Calls to the Help Desk related to virus attacks will be logged for analysis by the Desktop and Workgroup Services group and Information Security Administration as needed.

5.10.2 Desktop and Enterprise Services Group

- The Desktop and Workgroup Services Group is responsible for ensuring that all workstations are configured to run virus protection software automatically on a regular basis. The virus protection software should scan files in memory each time the workstation is started. The software should monitor files for virus infections each time they are opened. Additionally, the virus protection software should allow Employees to perform scans on diskettes and files, as they are loaded on to their workstations.
- The Desktop and Workgroup Services Group is responsible for ensuring that virus protection software is current and contains the latest vendor updates.
- The Desktop and Workgroup Services Group is responsible for reacting to all virus incidents reported by the Help Desk in a timely manner.



Corporate Information Security Confidential

- The Desktop and Workgroup Services Group must ensure that virus software is installed and active on all Servers.

5.10.3 Information Security Administration

Information Security Administration will monitor virus occurrences and make recommendations for future prevention. Additionally, Information Security Administration will communicate virus protection issues to all Employees via the security awareness program.

5.10.4 Virus Protection Software

- The first line of defense against virus infections from diskettes is to scan all incoming diskettes when they are first inserted into a workstation diskette drive. Additionally, the first line of defense for incoming files is to scan each file immediately after downloading. Each workstation must be equipped with anti-virus software for this purpose.
- Software distribution to networked workstations must be accomplished via standard distribution methods determined by the Desktop and Workgroup Services Group. Distributed software must be scanned for virus infection prior to distribution.
- Current versions of virus scanning software must be installed on each network server and automatically scan all files and directories on a periodic schedule.
- The anti-virus software installed on E*TRADE FINANCIAL workstations must provide Terminate Stay Resident (TSR) capabilities that monitor for suspected virus behaviors during normal use.

It must be noted that there is no 100% protection from virus threats. However, by following the above policy, the risk of serious virus incidents is significantly reduced. To further insure against loss due to virus attack, information must be backed up as outlined in the Personal Computer Back Up Policy.

5.11 CELLULAR COMMUNICATION POLICY

Frequent and rapid communication between Employees of E*TRADE FINANCIAL is required to support many business objectives. E*TRADE FINANCIAL does not provide cellular telephones to its Employees. Employees with a business necessity may purchase their own cellular telephones and may expense business-related calls in accordance with the reimbursement requirements set forth by the Finance Department. In lieu of cell-phone use, there are alternative communication channels that may be more effective:

- Regular Telephone
- Pagers
- Voice Mail
- Email
- Internal Instant Messaging

Each communication method can be used to support specific business requirements. The choice of the most effective method to support business objectives is dependent on many factors and represents a balance between cost, efficiency and convenience. Good judgment should be exercised in deciding how to reach someone urgently. The following factors must be considered when selecting a particular method:

- Security—Eavesdropping to intercept confidential and sensitive information is a possibility with analog cellular technology. Additionally, fraudulent use of cellular technology represents a significant economic risk to E*TRADE FINANCIAL.



Corporate Information Security Confidential

- Cost—it is significantly more expensive to use cellular telephones than other methods.

The following policies apply to Employee use of cellular technologies.

- Cellular communications must be kept to a minimum. Where appropriate, the use of regular telephones, pagers, or e-mail is preferred.
- Employees who fail to adhere to E*TRADE FINANCIAL cellular use policies may be held accountable for unauthorized charges.

5.12 REMOTE ACCESS POLICY

5.12.1 Dial-Up/Broadband Internet Services

Remote access via telephone dial-up/broadband Internet services to E*TRADE FINANCIAL computer environments is required to support certain business functions and specific technical objectives. Remote access also creates an additional point of entry into E*TRADE FINANCIAL's computer environments, and therefore requires control mechanisms to ensure that this access method is secure. This policy is intended to define secure authorized dial-in/broadband access, create a secure connection that is easy and unobtrusive for users, allow centralized accounting and management, and augment all other security perimeter requirements.

Remote users must be authenticated through a two-factor authentication server before they are granted access to E*TRADE FINANCIAL information assets. Two-factor authentication identifies an approved user by verifying both something unique that they have, such as a file or token number, and also something they know, which is usually a password. For stationary, known remote locations between unattended network resources such as servers and routers, dial-back authentication can be used in lieu of two-factor authentication. Authentication should be accomplished via an approved authentication technology, such as SecureID, a smart card, digital signatures, etc. In addition, remote passwords must conform to E*TRADE FINANCIAL's Password Policy.

Authentication must not be sent in the clear. In general, passwords should never traverse any network in unencrypted form. The passwords must utilize strong encryption (not encoding). Examples of acceptable encryption methods are: DES-56, TDES, RSA-512 or stronger. All remote connections utilizing the standard VPN client must have a properly installed firewall technology protecting its Internet connectivity. An approved firewall technology can be either a hardware or software solution.

5.12.2 Mobile Devices

Sensitive customer and company information is sometimes required for remote productivity; however, it should not be unprotected or retained on mobile devices such as laptops, PDAs, Blackberries, Smart Phones, etc. Sensitive documents must be encrypted using an encryption application approved by Information Security Management. Mobile users should regularly purge their devices of company information such as database extracts, logs and audits, email, memos spreadsheets, etc.

All E*TRADE FINANCIAL laptops must have Credant Technologies' Mobile Guardian client to assist in securing data on mobile devices by encrypting all computer media, file and application data. Any exemption to this policy requires a MAC request listing the business reason and must be approved by Corporate Information Security.

Mobile devices are most vulnerable to theft; therefore mobile devices should not be left unattended in vehicles, airports, etc for any reason.



Corporate Information Security Confidential

Laptop computers should not be left unattended in offices, hotel rooms, etc without the use of a cable lock.

Mobile devices should be used with the password feature enabled.

5.12.3 General Remote Access Requirements

- There are 2 approved methods of remote access - Citrix and VPN.
- All systems connecting via VPN must use anti-virus and software firewall solutions approved by Information Security Administration and managed by E*TRADE FINANCIAL.
- Non-E*TRADE FINANCIAL equipment connecting via VPN requires the use of a hardware firewall device in addition to E*TRADE FINANCIAL managed anti-virus and software firewall solutions and must be approved by Information Security Administration.
- Written authorization requests for remote access must be made by the manager of the business area for each employee requiring access. The authorization request must include the business reason for the request. In addition to authorization, approval for the access must be granted by Information Security Administration.
- Remote access to system resources will be granted on an as-needed basis and will be in line with user job responsibilities. Anonymous, guest or generic access is prohibited. In addition, broad and/or unlimited access is prohibited.
- Access will be granted in a timely manner upon receipt of a properly documented request by Information Security Administration. Conversely, access must be removed immediately for individuals that are reassigned to other job responsibilities not requiring access or upon termination of employment or business relationship.
- Information extracted by remote access requires the same degree of protection employed for other classified E*TRADE FINANCIAL information.
- Dial-up telephone numbers are considered confidential information and their unauthorized disclosure is prohibited. Periodically, remote access telephone numbers will be changed to new numbers.
- Accountability, responsibility and authority are established for remote access by assigning specific user accounts for each authorized individual. Generic authorizations are prohibited.
- Host response to access requests must not acknowledge or return additional request parameters to the requesting system. Instead, the requesting system should supply all identification and authentication information without prompting.
- All remote access sessions must be logged to satisfy audit requirements. Log files must be maintained in a secure environment.
- Remote access connections must be terminated after a specific period of inactivity during any active session.
- Connections for invalid access attempts must be terminated after five invalid login attempts.

5.13 ENCRYPTION POLICY

Encryption is used to ensure the integrity of E*TRADE FINANCIAL data and to control access to confidential data. Data classified as **"Customer Confidential or Company Sensitive"** shall be encrypted while traversing the Corporate Wide Area Network (WAN) and customer web server communications. Encryption shall use a key length compatible with current technological needs, as defined by Information Security Administration (minimum 56bit key). The user must not be allowed to use a smaller key but they may be allowed to use a larger key. Keys will be assigned to only one user and they may not be shared among users. There must be no way for another key to retrieve the data.



Corporate Information Security
Confidential

5.14 PHYSICAL ACCESS POLICIES

5.14.1 General Physical Access Control

- Access to offices, computer rooms, and work areas containing sensitive, valuable, or confidential information resources (i.e., customer information, Human Resources files, documentation, and other types of internal information), in any form (electronic, paper, etc.) should be physically restricted.
- All users are required to be authorized by management before entering E*TRADE FINANCIAL's facilities which may contain sensitive, valuable, or confidential information resources. Users are to be authorized only to those facilities required to perform their job functions.
- Hard-copy sensitive, valuable or confidential information should not be left in areas where it might be observed or discovered by unauthorized individuals. Whiteboards should be erased after each use. Confidential or sensitive documents should not be left on desktops, printers, copy machines, or fax machines.

Questions concerning physical and environmental controls should be directed to Corporate Safety and Security.

5.14.2 Handling of Sensitive Information

- Customer confidential or company sensitive information resources (i.e., customer information, software, documentation, and other types of internal information), in any form (electronic, paper, etc.) may be transferred from a regulated E*TRADE FINANCIAL's business unit to a deregulated business unit in electronic or hard copy form only after two conditions have been fulfilled. For this data transfer to take place a clear business need should exist AND advance permission from the information owner should be obtained.
- Hard-copy customer confidential or company sensitive information should not be left in areas where it might be observed or discovered by unauthorized individuals. This includes papers on a desk, in public areas, or papers which have been discarded. Customer confidential or company sensitive information should be properly discarded into an appropriate secured container for shredding. All such disposal, however, must comply with the Company's Records Management Policy, which is found on the Legal Affairs Department web page on Channel*E.
- Before any customer confidential or company sensitive information resources may be transferred from one computer to another, the person making the transfer should ensure that access controls on the destination computer are commensurate with access controls on the originating computer. If comparable security cannot be provided with the destination system's access controls, then the information should not be transferred.
- Customer confidential or company sensitive information resources (i.e., customer information, software, documentation, and all other types of internal information), in any form (electronic, paper, etc.) must not be sold or otherwise transferred to any non-E*TRADE FINANCIAL's party for any purposes other than business purposes expressly authorized by management.
- If customer confidential or company sensitive information resources are lost or disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties, the data owner and Information Security Administration must be notified immediately.

Management reserves the right to censor any data posted to Company computers or networks. These facilities are private business systems, and not public forums, and as such do not provide First Amendment free speech guarantees. E*TRADE FINANCIAL reserves to take whatever



Corporate Information Security Confidential

action it deems appropriate for violation of these policies, up to and including termination, civil and/or criminal action

5.15 DATA, DOCUMENTS AND E-MAIL RETENTION, ELECTRONIC AND PAPER

Data, documents and e-mail must have a lifetime. Limiting retention will save E*TRADE FINANCIAL the expense of storing large amounts of expired data for extended periods of time. Corporate, non-production systems to retain data for 30 days to allow for data recovery of failed systems and procedures. All documents and other forms of data must be retained according to the Company's Records Management Policy and the retention schedules applicable to various business units. The policy and schedules are accessible on Channel E* via the Legal Affairs Department webpage.

Electronic data must be securely removed from all storage devices when taken out of service. There are two approved methods for disposal: physical destruction or data overwrite. Either method is acceptable and must be sufficient to prevent recovery of the data.

Proper overwriting requires that the data be overwritten enough times that the data is no longer recoverable. Overwriting should use random characters for a total of 3 complete rounds to ensure confidential data cannot be recovered using conventional forensic technologies and must be done in a manner approved by Information Security Administration.

Proper physical destruction of data media requires that the physical media be destroyed to the point that it can no longer be used in any device to recover the data.

5.16 CUSTOMER DATA USE IN DEVELOPMENT & TESTING

To prevent unauthorized access to customer data, actual customer data should not be used for development or testing efforts. Artificial data should be generated for use in these areas.

5.17 EMBEDDED LINKS IN EMAIL COMMUNICATIONS

Embedded Web Links (URLs) should not be used in email communications with our customers to help protect against 'phishing'. Phishing is a type of attack where malicious emails are sent to our customers posing as E*TRADE FINANCIAL. Phishing emails are used to get customers to click on false links that facilitate the theft of their logon credentials, username and password. Customers should not consider email with embedded links as legitimate communication from E*TRADE FINANCIAL.

VI. SUMMARY OF SIGNIFICANT FEATURES

Scope: Security policies apply to all information infrastructures. The scope is intended to be broad rather than narrow.

Compliance: The policies are not optional. All Employees, contractors, temporaries and business partners are expected to comply.

Exceptions: It is recognized that deviations from policy may be necessary from time to time. An exception requires documentation, Management, and Corporate Information Security approval. Also, an exception for a limited purpose does not constitute a waiver of the policy, either in whole or in any other part.

Strategies: Basic security strategies include accountability, need-to-know, segregation of duties, separation of environments, defense in depth, auditing, monitoring and awareness.

Principles: There are four basic security principles adopted by E*TRADE FINANCIAL. They are: all information is owned by a specific individual; sensitive information must be classified; all